16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Title of Paper
Shared Awareness in Times of Crisis: A Framework for Collaboration

Topic(s)
Collaboration, Shared Awareness, and Decision Making; Approaches and Organizations; Concepts, Theory, and Policy

Name of Author(s)
Elizabeth Avery Gomez, Ph.D. and Paul Ray

Point of Contact
Elizabeth Avery Gomez, Ph.D.

Name of Organization
New Jersey Institute of Technology
University Heights GITC 4106
Newark, New Jersey
elizabeth.avery@njit.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Shared Awareness in Times of Crisis: A Framework for Collaboration	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **New Jersey Institute of Technology,University Heights GITC 4106,Newark,NJ,07102**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT
Shared awareness improves collaboration between actors in crises and can assist in overcoming issues related to motives, privacy and security. Strict adherence to the policies and procedures of parent organizations or teams during crises is often restrictive to effective collaboration and may be improved through shared awareness. For example, the Department of Defense (DoD) developed an information sharing strategy which aims to ?provide a common vision to synchronize initiatives to share information among DoD components, all levels of US government, international coalition partners, and the private sector and also supports the national strategy on information sharing? (DoD, 2007). We argue that shared awareness is needed to expedite and increase effective response during times of crisis as well as bypass the bottlenecks relating to motives, privacy and security, especially when these issues are related to or driven by non crises policies and procedures. A framework to support this research is needed and will be discussed. Concepts such as optimized information sharing, trust and interdependencies associated with effective collaboration will be examined to support the development of a framework.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**26**	

Shared Awareness in Times of Crisis: A Framework for Collaboration

ABSTRACT

Shared awareness improves collaboration between actors in crises and can assist in overcoming issues related to motives, privacy and security. Strict adherence to the policies and procedures of parent organizations or teams during crises is often restrictive to effective collaboration and may be improved through shared awareness. For example, the Department of Defense (DoD) developed an information sharing strategy which aims to "provide a common vision to synchronize initiatives to share information among DoD components, all levels of US government, international coalition partners, and the private sector and also supports the national strategy on information sharing" (DoD, 2007). We argue that shared awareness is needed to expedite and increase effective response during times of crisis as well as bypass the bottlenecks relating to motives, privacy and security, especially when these issues are related to or driven by non crises policies and procedures. A framework to support this research is needed and will be discussed. Concepts such as optimized information sharing, trust and interdependencies associated with effective collaboration will be examined to support the development of a framework.

Keywords: Collaboration, shared awareness, decision making.

Introduction

Establishing shared awareness between individuals, teams and organizations poses many challenges. The challenges increase when the actors have distinct modes of operation yet need a shared awareness to successfully solve a problem. Civil military operations (CMO, 2008) are one instance where organizations with distinct roles must establish at minimum a shared common operational picture (COP). The standards supporting COPs do not necessarily incorporate shared awareness. In fact, a shared awareness is a more detailed and complex approach to collaboration that requires a mutual application of context. One example of how a COP can improve but fail to optimize entity partnerships was the civilian-military collaboration effort after the 2010 earthquake in Haiti. Civilian web based technologies were able to identify and guide military operations toward areas of high need; however, issues related to motive, security and privacy often driven by established military policy and procedure, reduced the effectiveness of such collaboration. While efforts continue to address information sharing, our research places emphasis on the vulnerabilities two or more entities encounter when collaborating in crisis management where timely response is needed.

In this paper we discuss the challenges in achieving shared awareness and then present a preliminary framework for collaboration. A framework for collaboration can be used to enhance information sharing, effective communication, and to provide early checks for vulnerabilities between two entities. Many aspects of a systems design need to work together in order to provide effective mechanisms that efficiently support collaboration. Establishing a framework is even more important when entities are very different and

"trust and common ground" (Davenport & Prusak, 2000, p.97) are required for information sharing.

Background - Common Motives as a basis for developing a Framework

Despite any organizational differences that may exist between the military and civilian entities, their efforts to collaborate (especially during emergencies) are sometimes driven by very common motives or "key properties of culture" (Weick & Sutcliffe, 2001, p.121) such as protecting lives and restoring (or improving) political and economic normalcy. The reasons for these common motives may have competing origins, however, establishing a few "core values" can lead to cross organizational resiliency "during periods of uncertainty" (Weick & Sutcliffe, 2001, p.124) . Some areas where advantages may be gained through military-civilian collaboration are through the military's expertise and extreme capacity in logistics and civilian resources in information technology.

Collaboration in a Civil Military Context

In order to develop a clear picture of how civilian-military collaboration might work and how such efforts can be improved, we can first seek to establish a firm definition of collaboration and then examine how collaboration might change during crises or when organizations with differing polices and procedures need to work together.

A survey of the American edition of The Oxford Desk Dictionary and Thesaurus (1997) provided the following list of words and phrases related to collaboration – "to work jointly"; "together"; "cooperate"; "with other organizations"; "other entities"; "with agency/organization which is not immediately connected." This crude attempt to code key associated words and phrases, gives an impression of collaboration being a type of extraordinary cooperation; something above and beyond day to day occurrence; a special effort. If we accept this amalgamated definition of collaboration, it can be argued that collaboration between civilian entities and the military involves the need to work together and share resources. We believe however, that the most effective collaboration requires the need to acknowledge differences or boundaries in areas that can inhibit collaboration such as lack of trust and ultimately establish true shared awareness. Acknowledging these barriers to true collaboration (that are driven by motives, privacy and security) is a first step to establishing protocols.

Civil-Military Collaboration – A Discussion

When similar actors attempt to collaborate in emergencies, concerns about motives, privacy and security may be more easily addressed through prior establishment of mutual crises related processes and policies. Divergence of processes and policies across organizations can however lead to greater complexity when trying to establish protocols that transcend boundaries. Some examples of this include differences in security requirements for resources and human resources practices. Policies and procedures can also be driven by culture. In this sense, the military is a far more closed culture than most civilian organizations and tends to use more closed systems.

Online portals by design allow for customized views of information depending on an individual's role. A portal also affords a "dashboard" perspective allowing for

centralization of resources. The U.S. Army's Knowledge Online portal is one example of a single portal access to a large number of systems. Using the same example where access is centralized and simplified within the portal, the inter-entity collaboration is limited. For shared awareness between entities, an alternate approach is needed, especially in cases where similar information can be presented in different formats (i.e. iderms and mypersonell). Multiple methods of treating or inputting information may be one of the issues here. For instance, military personnel may input data valuable to the incident that is unclassified yet their only vehicle for data capture is the portal. Without a shared system, the external entities will be unable to view that information.

The above example also is sensitive in nature for political/cultural reasons beyond this paper. We note that getting past this cultural divide through re-engineering of procedures to "reduce (manual) checks and controls" (Hammer & Champy, 2006, p.61) is one key to establishing an effective framework for military-civilian collaboration. The possibility of even stronger cultural barriers must be considered if we are to apply our framework to a multi-national collaborative environment. Despite multi-national military operations and formal collaborations such as the ongoing war in Afghanistan and the North Atlantic Treaty Organization, formal civil-military collaboration continues to be rare outside of emergency events. Even within emergency events, the inter-entity sharing is challenged by information sharing policies.

A Shared Awareness Framework – Preliminary View

Developing a framework that is flexible enough to deal with the unique dimensions of crisis management is an ongoing challenge. This paper presents four initial steps towards a Shared Awareness Framework: 1) leverage CMO best practices; 2) establish shared awareness; 3) integrate management concepts such as process optimization; and 4) develop cross-national teams.

Step 1 – Leverage CMO Best Practices

We can borrow best practices from both civil and military organizations to determine what an effective framework for collaboration would look like. In fact, many procedures (if not policies) that exist in both types of organizations have adopted from traditional practices in the other. Examples of this adoption can be found in areas such as supply chain management, communications technology and the concept of "dash-board" monitoring systems or operations centers that may access shared databases (Hammer & Champy, 2006, p.96). One key aspect then of developing effective civil-military collaboration, is to develop hybrid protocols of collaboration that focus more on an "organizational capabilities framework" (Christensen, 2006, p.186) and policies than the tools or technologies that are already similar. For instance, Gomez and Chimento (2011) discuss the importance of "raw data" that is pure in contrast to "information" which has been processed by intelligence experts. Using raw data for hybrid protocols would allow for key elements of an incident to be shared without the interpretation of the internal (military) organizations intelligence experts.

Step 2 – Establish a Shared Awareness
Shared awareness is the second tier of importance in developing an effective civil-military framework for collaboration. Civil and military entities alike place significant importance on the ability to provide a common picture to organizational stakeholders. True shared awareness may only be possible when effective protocols are in place that allows each organization's systems to speak to the others in a way that expedites the creation of a common picture. Establishing a standard of what this common picture looks like may help us to further understand what protocols need to be put in place.

Step 3 – Integrate Management Concepts
The third tier of our civil-military framework is the application of management concepts to improve efficiencies, eliminate inefficiencies and assist with optimizing the design of a framework for collaboration. Techniques such as decision analysis, optimization and reengineering can be applied at different stages of the framework development or operation to improve effectiveness.

Step 4 – Develop Cross-Organizational Teams
The fourth and final tier of our framework is related to the effective development of cross organizational teams. One area of importance in developing strong teams is continuity. In the absence of continuous real world experience, strong teams require constant training and practice. Traditional obstacles to training and practicing together have been overcome by web-based technologies that eliminate location and resources limitations.

Protocols for Information Sharing - A Discussion of Motives, Privacy and Security
Information sharing between organizations inevitably raises questions about motives, privacy and security. Establishing clear protocols based on motives, privacy and security is one way to address these questions. By examining possible approaches to developing such protocols, we may be able to create an effective, expedient information sharing environment.

We previously discussed common motives as a basis for developing an effective civil-military framework for collaboration. Using common motives which support the mission at hand as the starting point for designing protocol can provide a clear picture of where civil-military collaboration can be most efficient and effective. The ability to remove personal motivators and entity specific perspectives allows for a pure view of the incident and goals to be accomplished. Decision analysis and optimization tools can be used to assist with determining the most effective protocol design when considering motives (goals) that are less common or unique to one organization.

Although privacy and security issues are common to both civilian and military organizations, there may be differences in how these concerns are managed. "Transforming work groups into authentic established teams" (Robbins & Judge, 2009, p.323) that train, work and communicate often together, along with adherence to an international security check standard may go some way toward working out the differences. Privacy and security protocols should also consider physical access to resources and planned alternatives when available resources or conditions are not ideal.

Conclusions and Next Steps

This research in progress places emphasis on shared awareness which differs from a common operational picture. We leverage Christensen's (2006) organizational capabilities framework as a first step. For effective collaboration in crisis management, we posit that a shared awareness is essential. Next steps of this research will illustrate the importance of a shared awareness.

References

1. Christensen, C.M., The Innovators Dilemma (2006), Collins.
2. CMO. Joint Publications 3-57. Civil Military Operations, July 8, 2008 http://www.fas.org/irp/doddir/dod/jp3_57.pdf
3. Davenport, T.H. & Prusak, L., Working Knowledge – How Organizations Manage What They Know (2000), HBS Press.
4. DHS. Secretary Napolitano Announces New Standards for Private Sector Preparedness, Department of Homeland Security, Press Release Date: June 15, 2010.http://www.dhs.gov/ynews/releases/pr_1276616888003.shtm
5. DHS. National Response Framework, January 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
6. DoD. United States Department of Defense Memo on Information Sharing Strategy Online, Office of the Chief Information Officer, May 4, 2007, Web April 5, 2011.
7. Gomez, Elizabeth A. "Towards Sensor Networks: Improved ICT Usage Behavior for Business Continuity". SIGGreen Pre-ICIS Workshop, December 2010.
8. Gomez, E. A. and Chimento, J., "Information Access Challenges: Data Fission Needs of the Field Expert," ICCRTS, June 2011.
9. Hammer, M. & Champy, J., Reengineering the Corporation – A manifesto for Business Revolution (2006), Collins.
10. Robbins, S.P & Judge, T.A. Organizational Behavior (2009), 13th edition, Pearson-Prentice Hall.
11. The Oxford Desk Dictionary and Thesaurus, American Edition (1997), Berkley Reference.
12. Weick, K.E. & Sutcliffe, K.M., Managing the Unexpected – Assuring High Performance in an Age of Complexity (2001), Jossey-Bass.

Shared Awareness in Times of Crisis: A Framework for Collaboration

Dr. Liz Avery Gomez and Paul Ray
New Jersey Institute of Technology

Motivation

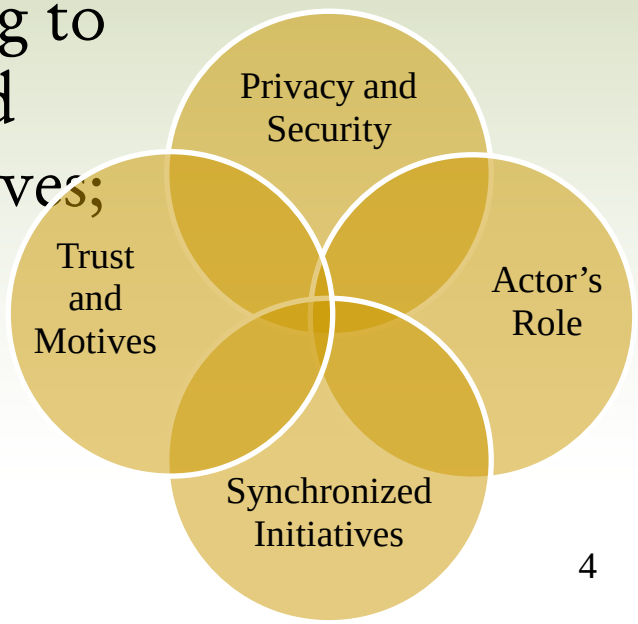
- Cross-organizational collaboration is a constant in any large scale disaster.
- Civilians who are in the affected area are the first to respond in a crisis.
- Local and global organizations respond accordingly.
- Achieving a shared awareness for efficient collaboration remains a challenge.

Overview of Today's Presentation

- Current view – challenges (disabilities)
  - Privacy and security
  - Trust and motives
  - Synchronized initiatives
  - Actor's role for the incident
- Proposed view – opportunities (capabilities)
  - Best practices
  - Shared awareness
  - Process optimization
  - Cross-organizational teams
- Towards a framework
- Information Communication Technology- next steps
- Conclusions

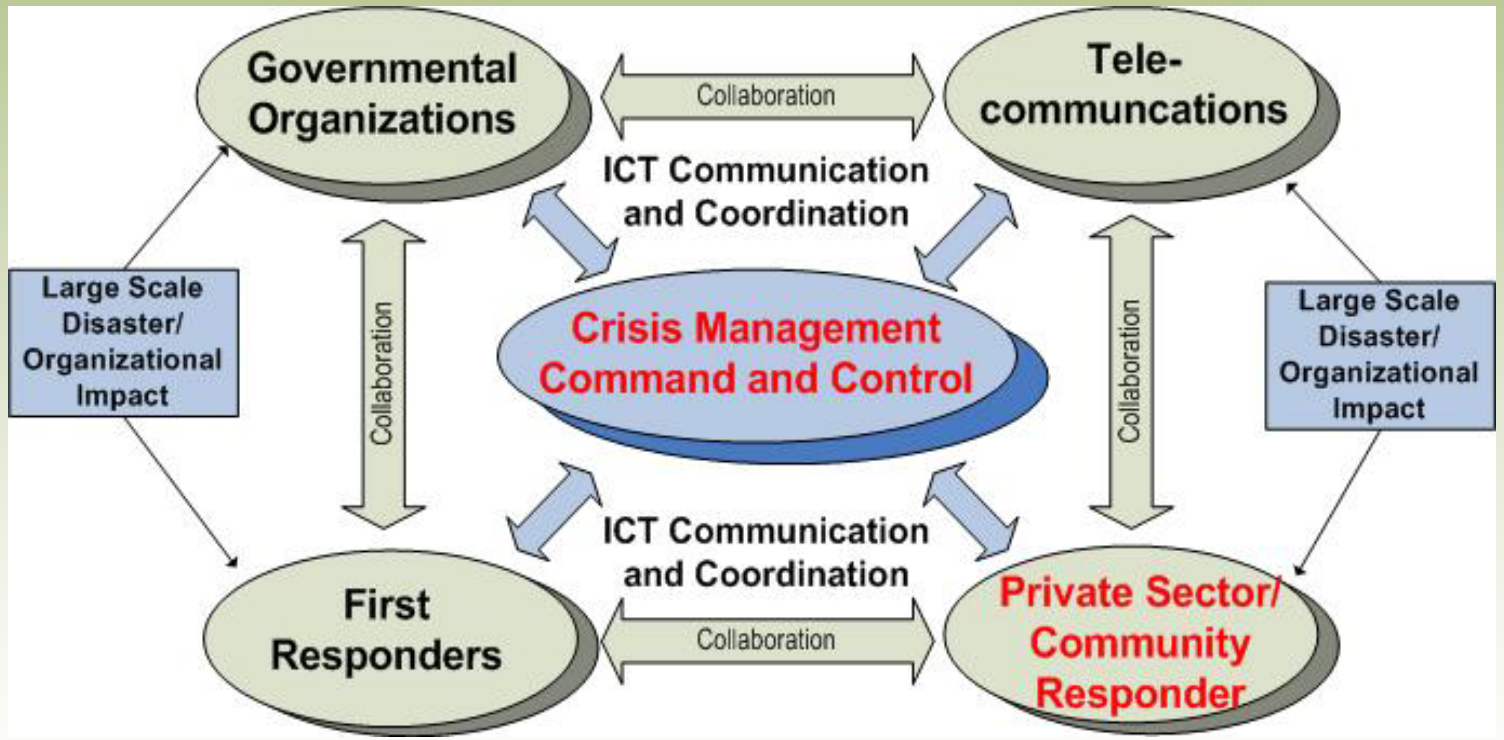
Research Objective

- To develop a civil military framework for collaboration in times of crisis.
- The framework should:
  - Support the national strategy on information sharing (DoD, 2007)
  - Bypass the bottlenecks relating to privacy and security; trust and motives; synchronized initiatives; and actor's role.



Civil Military Operations-Landscape

- CMO involve the organizational structures shown below:

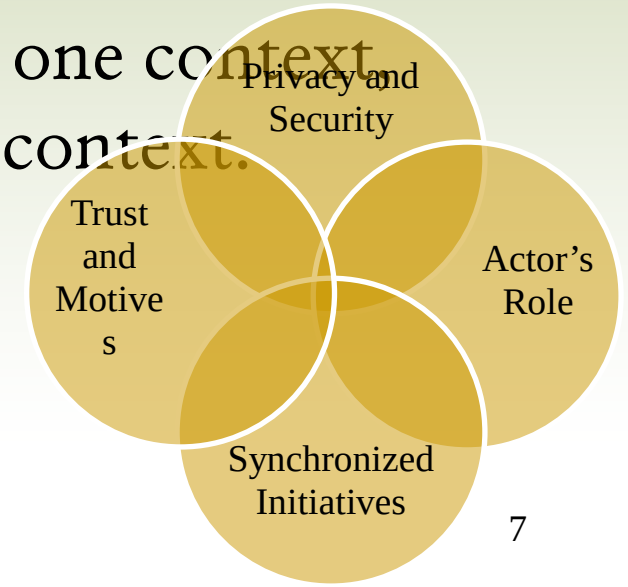


Capabilities and Disabilities

- Christensen (2006) notes the differences between the capabilities of people and capabilities of organizations where:
  - Processes are methods by which people have learned to transform inputs of labor, energy, materials, information, cash and technology into outputs of higher value
  - Organization's values (criteria that managers and employees in the organization use), are intrinsic when making prioritization decisions.

Opportunities from Capabilities

- People are quite flexible, in that they can be trained to succeed at different things.
- Processes and values are not flexible and can be ineffective when used in the wrong context.
- The very processes and values that constitute an organization's capabilities in one context define its disabilities in another context.



Privacy and Security - Process

- Organizations have their own guidelines for privacy and security
- Intranets with portal functionality are effective ways to manage privacy and security internally
- Information systems with broadband access enable internal privacy and security and facilitate shared awareness.

Trust and Motives for Civil Military Operations - People

- Getting beyond the cultural divide through "re-engineering" to reduce (manual) checks and controls (Hammer & Champy, 2006)
- Efforts are driven by common motives and key properties of culture (Weick & Sutcliffe, 2001).

Synchronized Initiatives - Process

- Establishing core values can lead to cross organizational resiliency during periods of uncertainty
- For CMO extreme capacity in logistics and civilian resources can be mitigated by information technology.

Actor's Role - People

- Differences between military roles and civilian roles vary greatly, especially with training and practices
- Military personnel might have access to centralized resources such as the "U.S. Army's Knowledge" online portal
- Non-military personnel would not have access to the same "knowledge".

Inhibitors to Cross-Organizational Collaboration

- Sustainable inter-organizational innovation becomes a disruptive innovation when moving from challenges to opportunities as follows:

Challenges - Disabilities	Inter-Organizational	Cross-Organizational
Privacy and Security	high security (portal)	blocks information flow
Trust and Motives	strengthen organizational goals	conflicting perspectives
Synchronized Initiatives	alignment of processes	inflexible processes
Actor's Role	effective work flow	distinct training paradigms

Proposed View - Opportunities

- Step 1 – Leverage Best Practices
- Step 2 – Establish a Shared Awareness
- Step 3 – Optimize Processes
- Step 4 – Develop Cross-Organizational Teams

Step 1 - Leverage Best Practices

- Identify traditional procedures and policies used by organizations
- Propose hybrid protocols (Gomez and Chimento, 2011)
- Consider physical access to resources and planned alternatives when constraints are present (Gomez, 2008).

Step 2 – Establish a Shared Awareness

- Identify key aspects of an incident that contribute to a common operational picture
- Expedite communication methods (speak freely)
- Increase training and practice to establish trust.

Step 3 – Optimize Processes

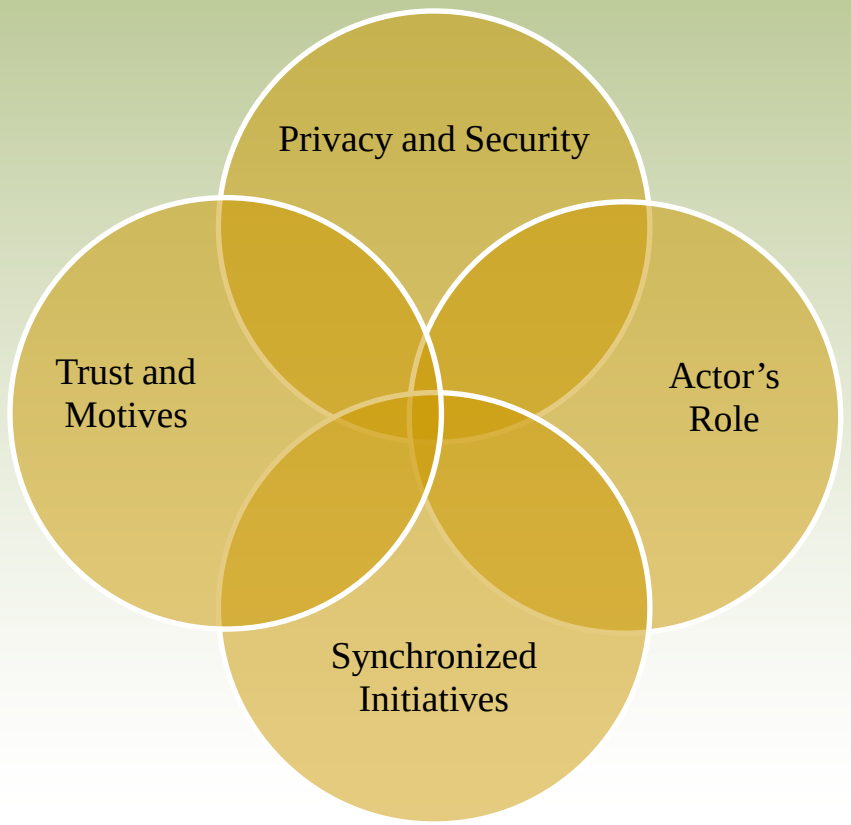
- Implement management concepts to improve efficiencies
- Include the use of information technology for decision analysis and process optimization.

Step 4 – Develop Cross-organizational Teams

- Establish a team structure that ensures the continuity of business
- Identify areas for continuous training and practice
- Remove personal motivators from incidents objectives
- Transform work groups into established teams (Robbins & Judge, 2009).

A Civil Military Collaboration Framework

Current View - Challenges



Proposed View - Opportunities

Information Communication Technology (ICT) – Next Steps

- Our focus since 2005 has been on training and practice
- We focus on the use of ICT straddling normal use to early crisis response (first 72 hours)
- We monitor ICT use of grassroots organizations and NGOs as they relate to military, public and private sector
- Our current focus is on process optimization and ways to institute best practices for cross-organizational collaboration providing a shared awareness.

Conclusions

- Our focus is on processes where sustainable inter-organizational innovation becomes disruptive innovation when confronted with cross-organizational collaboration.
- Our current research focuses on hybrid protocols that address the "data" needed for a shared awareness.